Australian Government

Digital Transformation Office

Third Party Identity Services Assurance Framework

Compliance Audit Guide

Version 2.0 December 2015

Digital Transformation Office

Licence

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the *It's an Honour* website (http://www.itsanhonour.gov.au)

Contact us

Enquiries or comments regarding this document are welcome at:

Assurance Framework Competent Authority
C/O Director, Trusted Digital Identity Team
Digital Transformation Office
Email: authentication@dto.gov.au

Contents

Figures

1. Guide Management

1.1 Change Log

This is the first published edition of the Third Party Identity Services Assurance Framework (The Framework) Compliance Audit Guide (ACAG).

1.2 Review Date

This document will be reviewed regularly and updated in line with changes to relevant government protective security policies, manuals and frameworks.

1.3 Conventions

This document adopts the following conventions:

- **MUST** indicates a mandatory requirement that a Service Provider is required to meet in order to satisfy a control test. This convention is also used to describe actions or activities to be undertaken by the Authorised Auditor.
- **SHOULD** indicates something that is not mandatory but is recommended which supports either a control test or is considered best practice.
- **MUST NOT** indicates something that if practiced, exercised or implemented will breach an Assurance Framework Accreditation requirement.
- **NON COMPLIANCE** will result if an Authorised Auditor determines a Service Provider does not meet a mandatory requirement listed in this document. Non-compliance severity ratings are listed at Annex A. A template for recording non-compliance is provided at Annex B.

1.4 Terms and Definitions

The terms and definitions used in this document are defined in the *Identity and Access Management Glossary*.

Note the following terms which are used extensively throughout this document.

Term	Definition
Compliance Audit	An engagement of an Authorised Auditor to conduct an independent audit to determine whether or not a Service Provider is compliant with an accreditation regime.
Authorised Auditor	Refers solely to an endorsed qualified ICT security professional listed on the Australian Signals Directorate Information Security Registered Assessors Program (IRAP) website. See the IRAP website for further information http://www.asd.gov.au/infosec/irap/assessors.htm

Term	Definition
Prior audit work	Refers to Payment Card Industry Data Security Standard (PCI DSS) audit work successfully completed in the period since the previous compliance audit (or since accreditation if undertaking the first compliance audit).
Service Provider	Refers to an accredited entity.

1.5 Advice on this Guide

Advice on the IRAP Guide or suggestions for amendment can be forwarded to:

Enquiries or comments regarding this document are welcome at:

Assurance Framework Competent Authority
C/O Director, Trusted Digital Identity Team
Digital Transformation Office
Email: authentication@dto.gov.au

1.6 Document Structure

This document is structured in the following manner:

- Section 2 provides an introduction to the Third Party Identity Services Assurance Framework Compliance Audit Guide.
- Section 3 describes the Assurance Framework audit process.
- Section 4 lists the compliance criteria and suggested audit guidance.
- Annex A: Non-Compliance Ratings list non-compliance severity ratings
- Annex B: Non-Compliance Template contains a non-compliance template that Authorised Auditors can use to record their findings for areas on non-compliance

2. Introduction

2.1 Purpose

Under the Third Party Identity Services Assurance Framework (Assurance Framework), annual compliance audits remain a condition of accreditation for Service Providers under the Assurance Framework accreditation. The Digital Transformation Office (DTO) requires that Authorised Auditors conduct an audit of Service Providers' compliance with the Assurance Framework on the anniversary of their initial accreditation date.

Failure to undertake an annual compliance audit represents a breach of the Assurance Framework Head Agreement/ Memorandum of Agreement and may result in termination of accreditation.

The primary objective of the ACAG is to provide a work program to assist Service Providers in meeting their compliance requirements. The ACAG provides guidance to Authorised Auditors on the scope and conduct of the assessment required under the Assurance Framework.

3. The Framework Audit Process

3.1 Audit Engagement

Service Providers **SHOULD** consider the following activities before engaging an Authorised Auditor:

- Develop a Statement of Work (SOW) which describes the audit work to be undertaken. Include any information relating to changes that have occurred in the Service Provider's operating environment in the period since the previous ACAG, including:
  - Outcomes of prior audit work;
  - Changes to Service Providers environment or Assurance Framework Approved Documents;
  - Changes in the ownership or management of the Service Provider or operating environment;
  - Compromises or security incidents;
  - Frequency of internal reviews; and
  - Outcomes from testing Disaster Recovery and Business Continuity plans or Incident Response procedures.
- Release the ACAG SOW with a Request for Tender (RFT);
  - Authorised Auditors may use information within the ACAG SOW to assist in drafting their response to the RFT.
- Review the responses to the RFT.
- Select an Authorised Auditor.
  - The Authorised Auditor **MUST NOT** be the same person used to undertake the IRAP before being accredited. This is to ensure that the person undertaking the assessment does not audit their own work.
  - Once an Authorised Auditor has been selected the successful respondent and Assurance Framework Competent Authority **SHOULD** be informed.
- Upon appointment, the Authorised Auditor:
  - Will define the scope of the assessment to be conducted in consultation with the Service Provider;
  - Will formalise a contract with the Service Provider to conduct the Audit;
  - Will perform the ACAG as required; and

Will report its findings to the Assurance Framework Competent Authority, the Service Provider and any other parties agreed between the Authorised Auditor and the Service Provider.

3.2 Prior Audit Work

This document provides guidance on how an Authorised Auditor may use the results of previous audit activities to reduce the possibility of duplication.

The Assurance Framework Competent Authority recognises PCI DSS as suitable commercial audit programs that can be considered by the Authorised Auditor as prior audit work.

An Authorised Auditor **SHOULD** review any PCI DSS audit work completed in the period since the previous Assurance Framework compliance audit. The Authorised Auditor is free to use their discretion in deciding whether to leverage the PCI DSS audit work.

Service Providers that have completed, or are considering A PCI DSS audit program are required to provide status reports to the Authorised Auditor.

Incorporating prior audit work by the Authorised Auditor provides a number of benefits to Service Providers:

- Continuity between audits so that continual improvements to the Assurance Framework operations may be realised;
- Ensuring that previous audit findings and recommendations are given due consideration in the subsequent audit;
- Reducing expenditure on external audit requirements due to overlaps in audit activity; and
- Reducing the extent of interruptions to operations when audits occur.

The ACAG does not unequivocally accept prior audit work as sufficient to meet the compliance requirements for the Assurance Framework. Rather, the *modular* structure of ACAG allows, where possible, work programs conducted under PCI DSS to be used as a substitute for parts of the ACAG work program. This is conditional on the Authorised Auditor being satisfied that the prior audit work provides adequate assurance within the constraints of the ACAG.

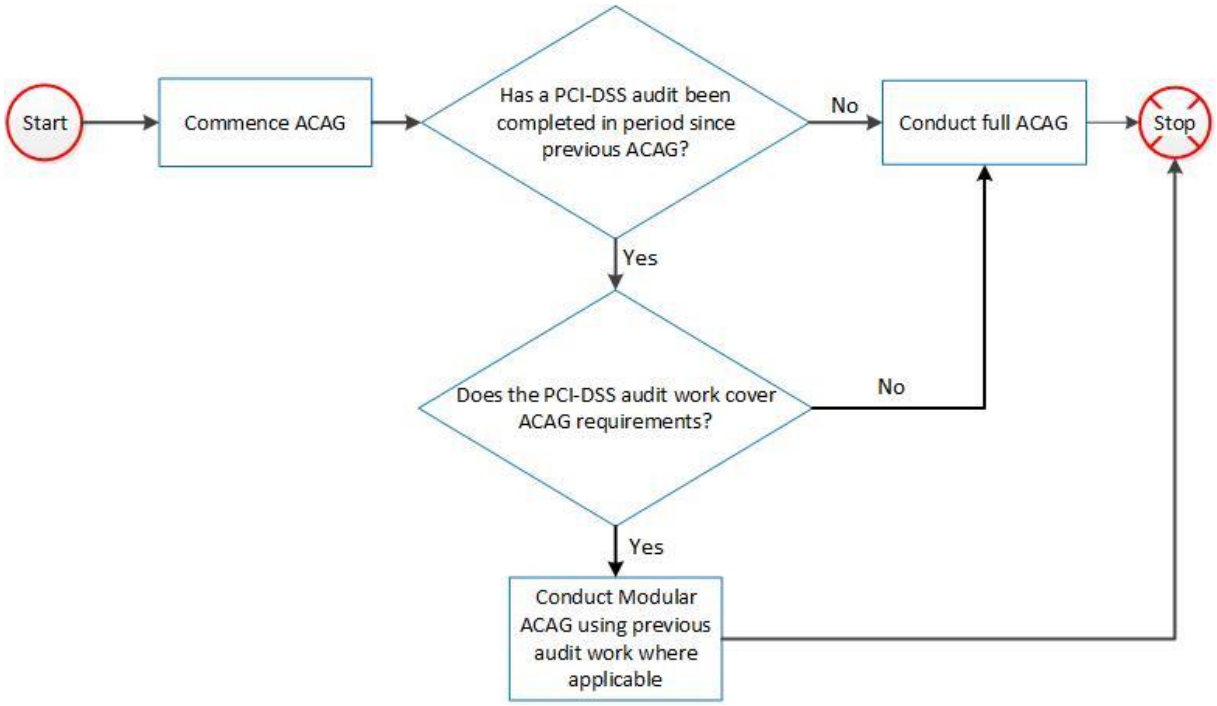
- For various reasons the Authorised Auditor may choose not to consider previous audit activity and conduct a full Assurance Framework audit. The Authorised Auditor and the Service Provider will discuss and agree the factors contributing to this assessment.
  - The Authorised Auditor may decide to conduct a full audit if prior work is deemed to be unreliable, insufficient or there is a lack of evidence of the nature of the work undertaken.
- The 'actual' PCI DSS audit work being considered **MUST** have been undertaken in the period since the previous Assurance Framework compliance audit (or since accreditation if undertaking the first Assurance Framework compliance audit), not the date on which the final Audit report was issued.

When a decision has been made to use work from a PCI DSS audit, the Authorised Auditor **MUST** ensure that the decision is adequately supported. If an Authorised Auditor decides that prior audit work will not be used, the Authorised Auditor **MUST** document the reasons why in the final audit report.

Figure 1 shows the key decision points that an Authorised Auditor **SHOULD** consider when planning the Audit of a Service Provider's operations. This will help Authorised Auditors to consider prior work performed.

A full ACAG is required if the Authorised Auditor chooses not to rely on any audit work performed since the previous ACAG.

Figure 1 Authorised Auditor – ACAG Planning Procedure



3.3 Documents to be reviewed as part of a full audit

The following Information Security Documentation **MUST** be reviewed by the Authorised Auditor as part of a full ACAG:

- Protective Security Risk Review (PSRR);
- Security Risk Management Plan (SRMP);
- System Security Plan (SSP), comprising;
  - Standard Operating Procedures (SOP);
- Physical & Environmental Security Plan (PESP);
- Personnel Security Management Plan (PSMP);
- Incident Response Plan (IRP); and
- Disaster Recovery and Business Continuity Plan (DRBCP).

3.4 Controls and waivers

A control is satisfied if the Authorised Auditor determines the Service Provider has successfully met the intent of a control. A control is not satisfied if the Authorised Auditor determines the Service Provider has not successfully met the intent of a control.

Where a waiver has been granted in relation to any aspect of a Service Provider's operations, the Authorised Auditor **MUST** sight the document and make allowance for the waiver in their evaluation and indicate this in the audit report.

The Authorised Auditor **MUST** comment on each instance of **NON COMPLIANCE**. Comments are to include an indication of the extent to which the Service Provider does not comply with the control under evaluation. The severity ratings of **NON COMPLIANCE** are listed in Annex A: Non-Compliance Ratings. A template for providing comments on areas of non-compliance is outlined in Annex B: Non-Compliance Template.

3.5 Audit Reporting

Upon completion of the ACAG, the Authorised Auditor will issue a final Assurance Framework Audit Report to the Assurance Framework Competent Authority, the Service Provider and any other entities agreed to in the ACAG contract. Unless otherwise specified in the contract between the Service Provider and the Authorised Auditor, an Assurance Framework Audit Report is considered to be sensitive commercial information and **MUST** be treated with the required level of security controls for their protection.

As part of the Assurance Framework Audit Report, the Authorised Auditor **MUST** detail:

- The work conducted including the outcomes of any control tests that were conducted;
- Any adverse issues identified, including potential control or procedural weaknesses;
- Areas of non-compliance and their associated severity ratings[1]; and
- Recommendations to remediate identified issues and non-compliances.

Completed Assurance Framework Audit Reports are to be sent to the Assurance Framework Competent Authority at the following address:

Assurance Framework Competent Authority
C/O Director, Trusted Digital Identity Team
Digital Transformation Office
Email: authentication@dto.gov.au

3.6 Audit Report Review

The specific process for dealing with the final Assurance Framework Audit Report findings is contained within each Service Provider's Assurance Framework Head Agreement/Memorandum of Agreement.

The DTO will review the Assurance Framework Audit Report findings and will subsequently issue either a:

- Statement to the Service Provider advising that its Assurance Framework Accreditation will be maintained; or
- Notice to the Service Provider specifying any adverse compliance audit findings and the required remedial actions (including timeframes to implement the remedial action) that will enable the Service Provider to maintain its Assurance Framework accreditation. Depending on the nature of the non-compliance, remedial action may include an additional compliance audit.

[1] Annex A lists the non-compliance severity ratings and their associated definitions.

4. Compliance Audit Criteria

4.1 Audit Assessment

The ACAG consists of 65 audit criteria which cover the protective security requirements specific for the Assurance Framework. Alongside the audit criteria is guidance that can assist the Authorised Auditor in determining the adequacy of a Service Provider's controls. Authorised Auditors are free to use alternative assessment methods to evaluate the adequacy of the Service Provider's controls.

Below is an example of ACAG control and assessment guidance.

Control	Assessment Guidance
Unevaluated products are not used unless the risks have been appropriately documented and accepted.	Seek evidence that the Service Provider is not using unevaluated products unless the risks have been appropriately documented and accepted. Review the Service Provider's Security Risk Management Plan.

4.2 Summary of Audit Criteria

The following table lists the controls to be evaluated.

Section	Audit Criteria	Controls
	Total Controls	**65**
4.3	Assurance Framework Approved Documents	7
4.4	Personnel Security	4
4.5	Physical and Environmental Security	4
4.6	Media and ICT Equipment Management	16
4.7	Access Control Management	12
4.8	Operations Security	12
4.9	Incident Management	5
4.10	Business Continuity Management	4
4.11	Outsourced Arrangements	1

4.3 Assurance Framework Approved Documents

Control	Assessment Guidance
Management, Publication and Communication 1. Assurance Framework Approved Documents are approved by management.	Obtain the latest copy of the Assurance Framework Approved Documents from the Service Provider and the date and approved version of the Assurance Framework Approved Documents from the DTO. Review the Assurance Framework Approved Documents to check if the version number and date are the same as those provided by the DTO. If the Assurance Framework Approved Documents have changed in the period since the previous Assurance Framework compliance audit (or since accreditation if undertaking the first Assurance Framework compliance audit), obtain evidence of the Service Provider's submission to the DTO for re-evaluation and the subsequent approval. If an amended Assurance Framework Approved Document has been submitted to the DTO for re-evaluation and has not yet been approved, detail the submission and any reason why it has not been approved.

Control	Assessment Guidance
Security Risk Management Plan 2. Security risks are identified, evaluated and managed by the Service Provider. 3. All accredited systems are covered by a SRMP. 4. Assets to be protected are identified. 5. Risk owners are identified for every security risk. 6. Security risk tolerances are specified. 7. Security risks deemed unacceptable are treated.	Verify that the Service Provider has a defined risk management process which includes responsibilities, assets to be protected, risk tolerance levels and approved treatment options for unacceptable risks. Determine when the last threat and risk assessment was undertaken. • Was this completed in the timeframe prescribed in the SRMP? • Were there any adverse findings? • Have all remediation actions been authorised and implemented? • If any remediation actions do not appear to have been implemented and the reasons are not given are they addressed as residual risks? • Have they been officially approved and signed off by risk owners or management?

4.4 Personnel Security

Control	Assessment Guidance
8. Employees undergo an appropriate employee screening, and where necessary hold a Security Clearance appropriate for their job requirements. 9. Employees and contractors (where relevant) receive appropriate annual security awareness education and training as relevant for their job function. 10. Training records for every -specific position are maintained.	Verify that all staff have undergone appropriate employee screening for their position. Verify that information security awareness, education and training programs have been established for employees and contractors (where relevant). • Are the programmes in line with the Service Provider's Assurance Framework Approved Documents? • Do they include training requirements and training procedures for each role? • Do they include re-training requirements and re-training procedures for each role? • Review training records to verify personnel maintain a skill level which enables them to perform their duties satisfactorily.

Control	Assessment Guidance
11. All information security roles and responsibilities are defined and allocated.	Verify that the authorisations and security clearance requirements necessary for system access are specified in the SSP. • Verify that the Service Provider has appointed a security expert, as an Information Technology Security Advisor (ITSA) or equivalent position. • Verify that the Service Provider has appointed an Information Technology Security Manager (ITSM) or equivalent position. • Verify that each accredited system has a system owner. Verify that standard procedures for all personnel with access to accredited systems include: • Requirements to notify the ITSM of any Cyber Security Incident as soon as possible after the Cyber Security Incident is discovered • Requirements to notify the ITSM of access to any data or systems they are not authorised to access. • Responsibilities for the protection of assets and for carrying our specific security processes are clearly defined. – Have staff been made aware of these obligations? – Have the procedures been tested so that they can be followed during an emergency, Cyber Security Incident or other adverse event?

4.5 Physical and Environmental Security

Control	Assessment Guidance
12. Security perimeters are used to protect areas that contain either sensitive or critical information or information processing facilities. 13. Secure areas are protected by appropriate entry controls to ensure that only authorised personnel are allowed access. 14. Physical protection against natural disasters, malicious attacks or accidents are designed and applied. 15. Networks are managed and controlled to protect information processing facilities and information in systems and applications.	Confirm the Information Security Documentation contains a PESP. Review the Information Security Documentation to verify that each physical and environmental security control detailed in the document is still in place and operating as intended. Verify that any instances of compromise or suspected compromise have been managed in accordance with the Information Security Documentation Obtain evidence that a review of physical and environmental security arrangements has been conducted in the period since the last compliance audit (or since accreditation if undertaking the first compliance audit)? • Examine the results of the last security review • Were there any adverse findings? • Have all remediation actions been authorised and implemented? Verify that all physical control tests and maintenance checks were conducted in the period since the last compliance audit (or since accreditation if undertaking the first compliance audit). Consider: • Alarm and physical security control systems. • Emergency response processes. • Intrusion detection and prevention systems. • Firewall rules. • Environmental and fire control systems. • UPS and power generators. • The number of telecommunication service providers used.

Control	Assessment Guidance
	Examine the results of these tests and checks. • Were there any adverse findings? • Have all remediation actions been authorised and implemented?

4.6 Media and ICT Equipment Management

Control	Assessment Guidance
Information classification and labelling 16. Information is classified in terms of legal requirements, value, business criticality and sensitivity to unauthorised disclosure, loss, or compromise. 17. An appropriate set of procedures for information labelling are developed and implemented in accordance with the information classification scheme adopted by the Service Provider. **Asset management** 18. Every asset is owned and subsequently controlled. 19. Asset owners review user access rights at regular intervals. 20. Assets associated with information and information processing facilities are identified, managed and protected to a commensurate classification or sensitivity level of the information being handled. 21. Rules for the acceptable use of assets associated with information and information processing facilities are identified, documented and implemented.	Verify that the Service Provider manages their assets in accordance with the requirements outlined in the Information Security Documentation • Has the Service Provider implemented handling procedures for the use of assets? • Has the Service Provider nominated a person to be responsible for the management and control of assets? • Identify this person and verify they are performing their duties in accordance with the Information Security Documentation. • Are assets labelled in accordance with the Service Provider's information classification scheme and documented procedures? • Do procedures exist for the classification, sanitisation, disposal, destruction or re-classification of assets? • Are inventories of sensitive or classified assets maintained? • Can staff account for all sensitive and classified ICT equipment and media? • Determine using asset handling procedures or other means if staff meet their security obligations when transporting media offsite and report any anomalies.

Control	Assessment Guidance
22. Procedures for handling assets are developed and implemented in accordance with the information classification scheme adopted by the Service Provider. 23. All items of equipment containing storage media is verified to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal or re-use. 24. Security is applied to off-site assets taking into account the different risks of working outside the Service Provider's premise. 25. Media is disposed of securely when no longer required using formal procedures. **Asset protection** 26. Media containing information is protected against unauthorised access, misuse or corruption. 27. Equipment is maintained to ensure its continued availability and integrity. 28. Equipment is suitably protected to reduce the risks from environmental threats and hazards and opportunities for unauthorised access. 29. Equipment is protected from power failures and other disruptions caused by failures in supporting utilities. 30. Power and telecommunications cabling carrying data or supporting information services are protected from interception, interference or damage. 31. Unattended equipment has appropriate protection.	Verify that a review of access rights to assets has occurred in the period since the previous compliance audit (or since accreditation if undertaking the first compliance audit). • If any remediation actions do not appear to have been implemented and the reasons are not given are they addressed as residual risks? Verify that equipment and media are adequately protected against typical information security threats.

4.7 Access Control Management

Control	Assessment Guidance
User access management 32. An access control policy is established, documented and reviewed based on business and security requirements. 33. Access to information and application system functions is restricted in accordance with the Service Provider's access control policy 34. A formal user registration and de-registration process is implemented to enable the assignment of access rights. 35. A formal user access provisioning process is implemented to assign and revoke access rights for all user types to all systems and services. 36. Employees and contractors are only provided with access to the network and network services that they have been specifically authorised to use. 37. Access to information and the application system functions is restricted in accordance with the access control policy. 38. The access rights of all employees, contractors and external party users to information and information process facilities is removed upon termination of their employment, contract or agreement, or adjusted upon change.	Review the Information Security Documentation to verify that an access control policy exists. Consider the controls in the Information Security Documentation relating to access control and verify that: • Information dissemination and authorisation (need-to-know, need-to-access principles) are enforced. • Consistency between the access rights and information classification policies of networks, assets and ICT equipment is maintained. • Access rights are formally managed. • Access rights are removed when no longer required. Examine the previous three months of statistical data relating to system access and: • Determine using event logging or other means if system access events have been recorded as described in the Information Security Documentation and report any anomalies, and • Determine over the same period if system access controls were operated as prescribed.

Control	Assessment Guidance
Authentication Credentials 39. Access to systems and applications is controlled by a secure log-in procedure 40. Strong passphrases are used for access to systems. 41. Multi-factor authentication is used for database administrators, privileged users, [2]Positions of Trust and remote access. 42. The allocation and use of privileged access rights is restricted and controlled. 43. The use of utility programs that might be capable of overriding system and application controls are restricted and tightly controlled.	Consider the controls in the Information Security Documentation relating to single and multi-factor authentication credentials and verify that: • Multi-factor authentication is used for database administrators, privileged users, Positions of Trust and remote access. • Passphrase policy complies with the Australian Government Information Security Manal requirements for passphrase management. • A review of privileged access rights has occurred in the period since the previous compliance audit (or since accreditation if undertaking the first compliance audit). • Users with privileged access rights are incapable of overriding system and application security controls. • The controls are operating as prescribed.

[2] A role of authority within an Organisation usually involving duties that require a higher level of assurance than that provided by normal agency employment screening. In some organisations additional screening may be required. Those in a position of trust have the ability to access especially sensitive information. Positions of trust can include, but are not limited to, ITSAs, administrators or privileged users

4.8 Operations Security

Control	Assessment Guidance
Strategies to Mitigate Targeted Cyber Intrusions (Top 4) 44. The ASD 'Top 4' mitigation strategies are implemented. 45. Note: the Top 4 mitigation strategies include: – Application whitelisting, – Patch applications – Patch operating systems, and – Restrict administrative privileges.	Verify that the Top 4 mitigation strategies are implemented. Inspect the application white list to determine if users can only execute a defined set of trusted applications. Also determine if the white list can be disabled by general users or users with privileged access. Verify that security patches and updates are implemented in accordance with the Information Security Documentation.
Standard Operating Procedures 46. Operating procedures are documents and made available to all users who need them to carry out their duties.	Review the Information Security Documentation to verify that SOPs are documented and communicated to staff. Verify that the SOPs are formally approved prior to release.

Control	Assessment Guidance
Change Management 47. Changes to systems are formally managed. 48. Changes to the organisation, business processes, information processing facilities and systems that affect information security are controlled. 49. Modifications to software packages are limited to necessary changes and all changes are strictly controlled.	Review the change management process and determine the adequacy of the controls implemented. Consider the following: • Are formal procedures implemented for proposed changes? • Are staff aware of their responsibilities in terms of managing change? • How are changes identified and categorised? • Where are proposed changes documented? • Are there separate processes for managing standard, urgent and emergency changes? • Are the security impacts of proposed changes assessed? • Are changes planned and tested prior to implementation in the production environment? • How are aborted changes managed (i.e. provisions for fall back) • How are the details of implemented changes communicated to relevant staff?
Backup 50. Backup copies of information, software and system images are taken and tested regularly in accordance with the Information Security Documentation. 51. Security controls are implemented to protect data transfers through communication facilities.	Review the Information Security Documentation to verify that a backup process exists. Verify that the backup process is tested in accordance with the Information Security Documentation. Verify that data transfers are conducted as prescribed in the Information Security Documentation.

Control	Assessment Guidance
System monitoring and event logging 52. Event logs recording user activities, exceptions, faults and information security events are produced, centrally stored and regularly review. 53. Logging facilities and log information is protected against tampering and unauthorised access. 54. System administrator and system operator activities are logged and the logs protected and regularly reviewed. 55. The clocks of all relevant information processing systems within an organisation or security domain are synced to a single authoritative reference time source.	Verify system monitoring and event logging is undertaken in accordance with the requirements defined in the Information Security Documentation. • What types of system events are logged? • How often are logs reviewed? • What types of events are considered suspicious activity? • What staff know how to handle suspicious log activity? Verify that monitoring and logging facilities are adequately protected Verify the retention period for audit log information retained in backup or archive is in accordance with the Information Security Documentation. Inspect the reference time source used for event logging and verify it is consistent with Information Security Documentation. If multiple time sources are used verify that they are synchronised across the environment.

4.9 Incident Management

Control	Assessment Guidance
56. Information security events are assessed to determine if they are to be classified as Information Security Incidents. 57. Information Security Incidents are reported through appropriate channels as soon as possible. 58. The Service Provider define and apply procedures for the identification, collection, acquisition and preservation of information which can serve as evidence. 59. Responses to Information Security Incidents occur in accordance with documented procedures. 60. Knowledge gained from analysing and resolving Information Security Incidents is used to reduce the likelihood or impact of future incidents.	Review the IRP and test the Service Provider's incident management controls. Verify that the incident response plan has been reviewed in the period since the previous compliance audit (or since accreditation if undertaking the first compliance audit), Verify the incident monitoring, management and response capabilities operate as prescribed in the Information Security Documentation. Interview staff to verify they are aware of their responsibilities when handling an Information Security Incident. • What would they do? • Who would they tell?

4.10 Business Continuity Management

Control	Assessment Guidance
61. The organisation determines its requirements for information security and the continuity of information security management during adverse situations, e.g. during a crisis. 62. The Service Provider has established, documented, implemented and maintains processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation. 63. The Service Provider verify the information security continuity controls at least annually to ensure they are valid and effective during adverse situations. 64. Information processing facilities implement with redundancy sufficient to meet availability requirements.	Obtain evidence that the DRBCP has been tested in the period since the previous compliance audit (or since accreditation if undertaking the first compliance audit). Verify that the outcome of DRBCP testing has been documented. Verify the last test included a full restoration of the Root CA servers, databases, keys and data and report any anomalies. Verify that if any remediation actions do not appear to have been implemented and the reasons are not given that they are addressed as residual risks in the SRMP. Interview staff and verify they are aware of their roles and responsibilities in the event of a disaster. Verify that training programs referenced in the DRBCP have been implemented in accordance with the documented procedures?

4.11 Outsourced Arrangements

Control	Assessment Guidance
65. All relevant information security requirements are established and agreed with each supplier that interact with, or provide IT infrastructure components for the Service Provider's operations.	Verify that agreements with external organisations referenced in the Service Provider's Assurance Framework Approved Documents are current and in place.

Annex A: Non-Compliance Ratings

Severity Rating	Definition
CRITICAL	An Authorised Auditor's determination that the Service Provider does not comply with essential protective security requirements of the Assurance Framework shall be classified as a critical failure. For example, the inappropriate storage of cryptographic keys, digital certificates or passphrases shall be classified as a critical failure.
MAJOR	An Authorised Auditor's determination that the Service Provider does not comply with significant protective security requirements of the Assurance Framework shall be classified as a major failure. For example, a Service Provider does not review their SRMP annually. Escalation of the problem to a critical failure shall be imposed if additional related events impact on the Service Provider's operations simultaneously.
PARTIAL	An Authorised Auditor's determination that the Service Provider does not comply with important protective security requirements of the Assurance Framework shall be classified as a partial failure. For example Standard Operating Procedures not implemented in a manner consistent with the System Security Plan. Escalation of the problem to a major failure shall be imposed if additional related events impact on the Service Provider's operations simultaneously.
MINOR	An Authorised Auditor's determination that the Service Provider does not comply with general requirements of the Assurance Framework shall be classified as a minor failure. For example broken links within publically available documents.

Annex B: Non-Compliance Template

Audit Criteria:	**{e.g. Assurance Framework Approved Documents, Operations Security}**				
Total Section Controls:	{number}	Compliant controls:	{number}	Non-compliant controls:	{number}
Authorised Auditor comments					
Control No	Severity Rating	Comment			
{control #}	{As per Annex A}				
{control #}	{As per Annex A}				
{control #}	{As per Annex A}				